

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕАЛИЯХ БИЗНЕС-ТРЕБОВАНИЙ РФ

ТЕМА 2

Структура бизнес-машины

Спикер: Ануфриев Иван



ЗАНЯТИЕ 2.4

Риски ИБ при аутсорсинговой модели ИБ



Условное разделение информации. «Метки» на слайдах *

«Машина-времени-Time-machine» Возвращаемся и освежаем знания с прошлых занятий.		«Назад в будущее» Анонсируем то, что будет сказано на следующих занятиях	Метки по Времени
			
Рабочий «экспертный» инструментарий «Expert tools»	Примеры рабочих документов, лучшие приемы, практики и примеры использования. «Best practice»		Метки по используемым инструментам и практикам
{ EXPERT TOOLS } 	{ BEST PRACTICE }		
Полезные мысли и выводы «Инсайты»	Соответствие требованиям, нормативная база и полезные формы по НПА	В нашем курсе, отдельно выделяется информация, относящаяся к типу «непрерывность бизнеса»	Метки по типу информации
{ INSIGHTS }	{ COMPLIANCE } 	{ BUSINESS CONTINUITY }	

Основные рассматриваемые вопросы первой части занятия



ВОПРОС 1

Баланс затрат и
рисков ИБ

ВОПРОС 2

Способы
обработки рисков
ИБ

ВОПРОС 3

Корпоративная
сервис модель

ВОПРОС 4

Своими
ресурсами
vs
аутсорсинг

ВОПРОС 5

MSSP
vs
SECaaS



Основные рассматриваемые вопросы второй части занятия.

ВОПРОС 2.1

**Основной чек-лист
(дорожная карта)**

ВОПРОС 2.2

Основные риски

ВОПРОС 2.3

**Защита
Конфиденциальность
Доступность**

ВОПРОС 2.4

**Уязвимости,
Идентификация,
Физическая
безопасность,**

ВОПРОС 2.5

**Комплаенс :
Финансовые
гарантии,
завершение
контракта**





Из предыдущего занятия про «баланс» между затратами на систему ИБ и закрываемыми рисками ИБ



Доказать эффективность использования бюджета – одна из основных целей руководителя ИБ

Риски ИБ

Затраты на
систему ИБ

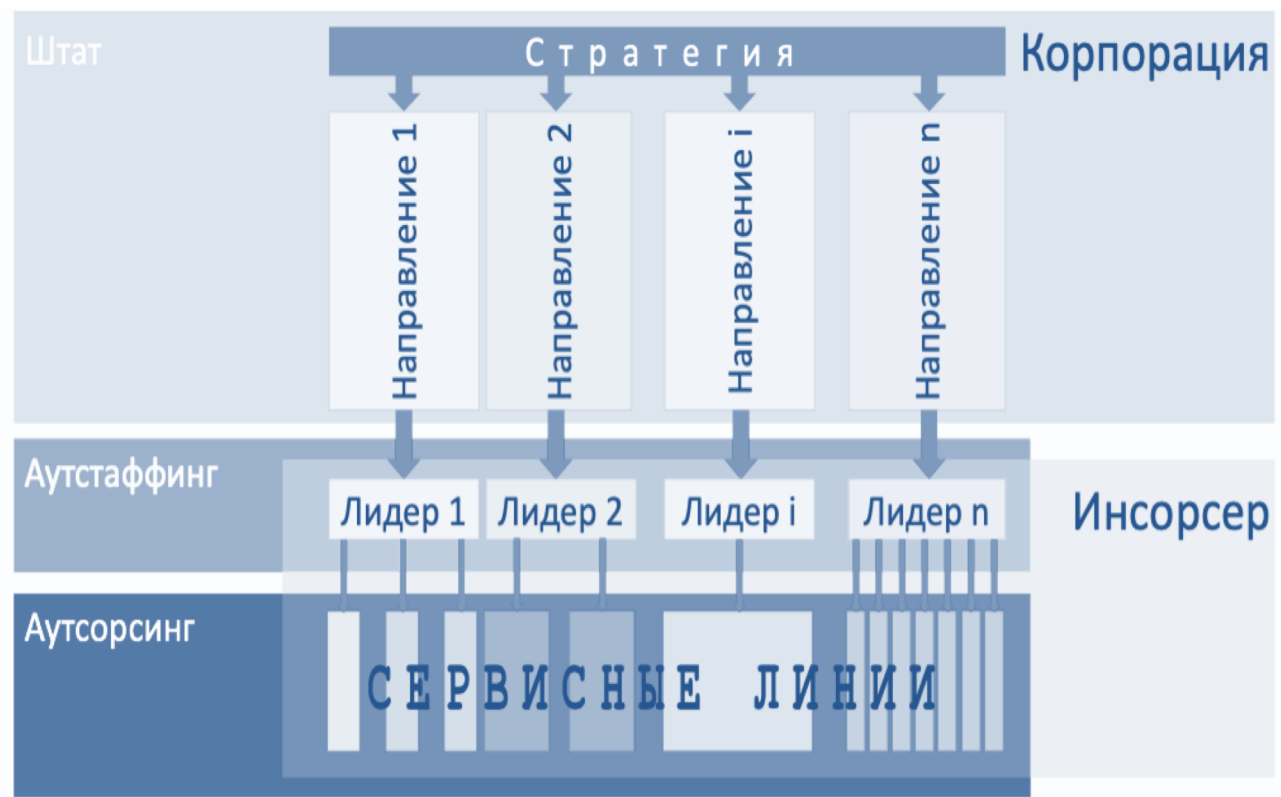


Обоснованный и
сбалансированный бюджет на ИБ

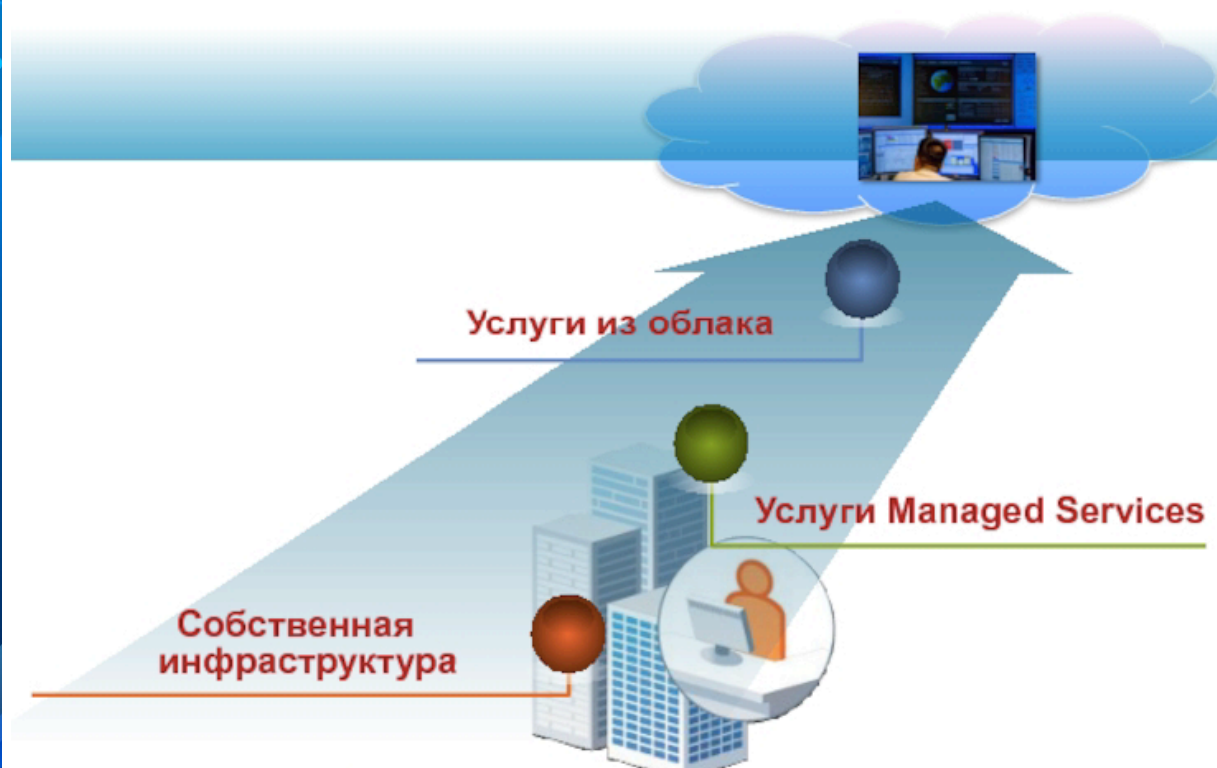




Вспомним про способы обработки рисков ИБ



Эволюция сервисов безопасности – от своего оборудования и сервисов до аутсорсинга классического и облачного



ПЕРЕХОД НА ОБЛАЧНУЮ МОДЕЛЬ ИТ

Было (инфраструктура)

Старые ИТ:

- Длинный жизненный цикл
- Стабильность и непрерывность
- Долгая реакция на запросы
- Низкая утилизация ресурсов
- CAPEX расходы

Стало (облачная модель)

Облачные ИТ:

- **Короткий time-to-market**
- **Фокус на скорости и гибкости**
- **Самообслуживание**
- **Равномерное использование ресурсов**
- **Расходы Pay-as-you-Grow**

Объем

Многообраз
ие

Скорость





Вспомним про корпоративную сервис-модель



Своя машина, такси *или* каршеринг ?



Самим обеспечивать ИБ,
получать сервис ИБ *или* получать конкретные услуги ИБ ?



Нельзя сравнивать по разным критериям: «холодное» и «мягкое»



Можно по разному владеть ресурсами
(ИТ/ИБ инфраструктуру или софт – можно приобрести или арендовать)

Также обслуживать по разным моделям
*(либо самим, если есть компетенции,
либо привлечь стороннюю компанию)*



Что такое аутсорсинг, какие вопросы задает Заказчик при выборе модели аутсорсинга ?

Аутсорсинг - это



Википедия
Свободная энциклопедия

Аутсóрсинг (от англ. outsourcing: (outer-source-using) использование внешнего источника и/или ресурса) — передача организацией на основании договора определённых видов или функций производственной предпринимательской деятельности другой компании, действующей в нужной области.



«В оригинале смысл слова “outsourcing” выражен словами “привлекать извне”. Для бизнеса это означает “передавать другой компании в поддержку часть функций собственного бизнеса»

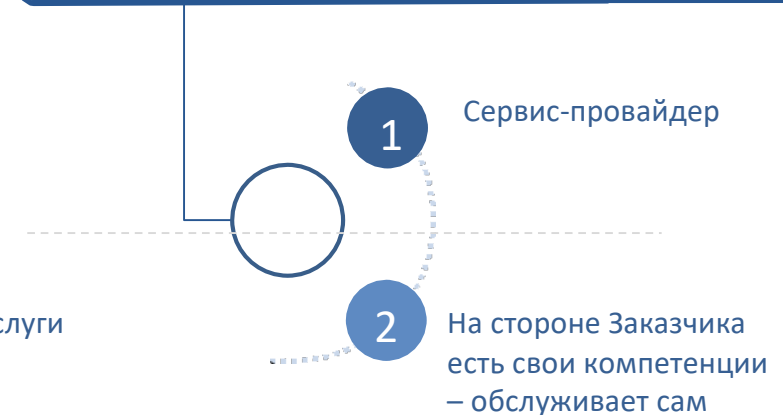
Чьи ресурсы (железо/софт) ?



Что покупает Заказчик ?



Если оборудование Заказчика, то кто обслуживает ?



Приняли решение перейти на аутсорсинговую модель.

Что дальше и что нас ждет ?

Классический аутсорсинг



MSSP (Managed Security Service Provider) – предприятие заказывает себе сервис ИБ (функцию), который будет предоставляться ей на базе некоего определенного набора средств защиты. Эксплуатацию данных инструментов берёт на себя MSS-провайдер.
Заказчику не требуется управлять настройкой самому.



MSSP – «водитель представляет Заказчику сервис доставки»



Облачный аутсорсинг

SECaaS (Security as a service) – предприятие покупает для себя конкретные услуги ИБ (технологии) в облаке сервис-провайдера с полной свободой в отношении применения средств управления.



SECaaS – «функцию управления берёт на себя Заказчик который управляет предоставленным ему оборудованием (транспортным средством)»



Основные рассматриваемые вопросы второй части занятия.

ВОПРОС 1

**Основной чек-лист
(дорожная карта)**

ВОПРОС 2

Основные риски

ВОПРОС 3

**Защита
Конфиденциальность
Доступность**

ВОПРОС 4

**Уязвимости,
Идентификация,
Физическая
безопасность,**

ВОПРОС 5

**Комплаенс :
Финансовые
гарантии,
завершение
контракта**





Основная дорожная карта при заключении контракта на аутсорсинг ИБ

для минимизации вероятности совершения инцидентов ИБ и тяжести их последствий



Защита данных и обеспечение конфиденциальности



Управление инцидентами



Управление уязвимостями



Ведение журналов регистрации
(в случае расследования)



Управление идентификацией



Физическая охрана и работа с сотрудниками



Уровень оказания сервиса



Безопасность приложений



Финансовые гарантии



Завершение контракта





Особенности договора и взаимодействия с сервис-провайдером

при заключении договора на аутсорсинг ИБ



Невозможность реализации большинства защитных мер со стороны Заказчика



Длительный процесс согласования



Со стороны Заказчика – смещение акцентов с обеспечения ИБ (в том числе реагирование) в сторону мониторинга и контроля



Аутсорсер должен соответствовать нормативным требованиям



Особое внимание со стороны Заказчика при работе с аутсорсером на юридических мерах и финансовой ответственности



Риски атак через подрядчика (supply chain attack)





Один из ключевых вопросов ИБ при выборе Заказчиком аутсорсинговой модели



Какая технология и какое конкретное место хранения наших данных у аутсорсера ?



Реализация контроля утечки данных



Как соблюдается конфиденциальность и целостность данных Заказчика, как данные отделены от данных других клиентов ?



Как и кто может получить доступ к личным данным клиента



Защита данных при их передаче



Удаление данных по завершении предоставления сервиса



Если для нас является критичной тематика обработки персональных данных – то данный вопрос является первоочередным



Обезличивание критичных данных и предоставление к ним доступа только авторизованному персоналу



Условия передачи данных клиента третьим лицам



Какие данные собираются о Заказчике ?



Гарантия нераскрытия информации третьим лицам



Где и как долго они хранятся данные Заказчика ?





Ключевой параметр, при заключении контракта с сервис-провайдером



Обеспечиваемый уровень доступности в SLA



Пиковые нагрузки и возможность аутсорсера справиться с ними



Меры обеспечения доступности, которое используются для защиты от угроз и ошибок (резервный оператор связи; защита от DDoS)



Доказательства высокой доступности аутсорсера



План действий во время простоя



Уровень сертификации ЦОД аутсорсера





Уровни уязвимостей



Как часто сканируется сеть ?



Процесс устранения уязвимостей



Возможность и условия осуществления внешнего сканирования сети с целью контроля защищённости заказчиком



Соблюдение требований облачного провайдера PCI DSS и ежеквартального сканирования ?





Необходимость подключения к системе без создания новых учетных записей



Возможность и устройство интеграции личным каталогом учётных записей



Поддержка SSO/MFA и предусмотренный стандарт



При наличии у аутсорсера собственной базы учётных записей необходимо учитывать процесс защиты и управления учётными записями



Поддерживается ли федеративная система аутентификации и какой под это предусмотрен стандарт ?





Уровень мер и процессы безопасности у сервис-провайдера не должен быть ниже, чем у Заказчика,



Какие предусмотрены режимные правила на объектах аутсорсера ?



Необходимо учитывать процедуру регистрации доступа персонала сервис-провайдера к данным Заказчика



В зависимости от задачи, важно учитывать, является ли инфраструктура выделенной или она разделяется с другими компаниями ?



Необходимо проанализировать результаты оценки внешнего аудита



Необходимо учитывать особенности процедуры набора персонала





Важно в случае, если Заказчик отдает на аутсорсинг приложения



Наличие приложения третьих фирм при оказании сервиса



Необходимо обратить внимание на исполнение рекомендаций OWASP при разработке приложений



Процедура тестирования для внешних приложений и исходного кода



Необходимо проверить использование мер защиты приложений, например: Web Application Firewall, Database Firewall, аудит БД





План действий аутсорсера в случае реализации инцидентов ИБ



Наличие плана реагирования на инциденты (включая метрики оценки эффективности)



Взаимосвязь политики управления инцидентами Заказчика и аутсорсера (особенно для зарубежных аутсорсеров, находящихся в другом часовом поясе)



Необходимо задокументировать все типы инцидентов, расставить приоритеты в инцидентах безопасности, проверить отчеты по проведению киберучений.



Необходимо учитывать возможные языковые барьеры, если аутсорсер находится за рубежом (при оперативном реагировании на инциденты времени искать переводчика не будет)





В случае потери журналов регистрации в электронном виде необходимо иметь дубликат на физическом носителе, который будет обновляться регулярно



В случае подключения третьих сторон, необходимо учитывать как аутсорсер обеспечивает сбор доказательств несанкционированной деятельности



Необходимо иметь информацию о том, как долго аутсорсер хранит логи и возможно ли увеличения этого срока



Также необходимо иметь информация о том можно ли организовать хранение логов во внешнем хранилище и как это можно организовать





Риски нарушения непрерывности бизнес-процессов являются ключевыми для предприятия



План обеспечения непрерывности бизнеса и восстановление после катастроф



Информация о наличии у аутсорсера резервного ЦОДа, в случае если аутсорсер прекратит свою деятельность или в случае если Заказчик решит не продлевать договор на оказание услуг



Информация о том, проходит ли аутсорсер внешний аудит по непрерывности бизнеса (наличие сертифицированных сотрудников по непрерывности бизнеса)



Что будет в случае если Заказчик решит не продлевать договор на оказание услуг, сможет ли он оперативно перейти к другому сервис-провайдеру ?





Важный момент, так как при обеспечении ИБ своими силами не всегда получается выявить и привлечь к ответственности виноватого



Необходимо иметь план действий в случае, если инцидент произошёл по вине аутсорсера.



Гарантия качества сервиса – описывается в SLA. Необходимо критически обдумать предложенные Заказчику метрики KPI



Необходимо понимать чем отвечает аутсорсер (то есть готовность аутсорсера возместить ущерб и посчитать его). Необходимо учитывать, что далеко не все компании активно пользуются киберстрахованием.



Далеко не каждый готов отвечать рублем



Нужно понимать какие финансовые гарантии подразумеваются в случае инцидента безопасности или нарушения соглашения об уровне сервиса (SLA) ?

1. Процент от упущенной выгоды;
2. Процент от заработка за время простоя;
3. Процент от стоимости информации, которая оказалась доступной в результате утечки;
4. Процент от суммы договора на оказание облачных услуг.





Разумеется, если она оформлена соответствующим образом



Кому принадлежат права на информацию, переданную аутсорсеру?

- А на резервные копии ?
- А на реплицированные данные ?;
- А на логи ?;
- А на приложения ?



Необходимо удостовериться, что заключенный контракт с Заказчиком не приводит к потере прав на информацию и иные ресурсы, переданные аутсорсеру





Думать о завершении контракта необходимо до его заключения



Необходимо учитывать процедуру выхода из контракта:

1. Как и в каком формате будет происходить возврат данных;
2. Как скоро будут получены мои данные обратно;
3. Как будут уничтожены все резервные и иные копии моих данных, а также как скоро это будет сделано и какие есть гарантии



Также нужно знать какие дополнительные затраты будут на завершение контракта



Готовы ли отдавать свои процессы информационной безопасности на аутсорсинг по моделям MSSP или SECaaS ?



**Благодарю
за внимание!**

